REMARKS

In response to the final action mailed August 5, 2008 and the Advisory Action dated October 23, 2008, the Assignee respectfully requests continued examination and reconsideration based on the above amendments and on the following remarks.

Claims 1-8, 11-29, 31-50, and 52-63 are pending in this application. Claims 9-10, 30, and 51 were previously canceled without prejudice or disclaimer.

Rejection of Claims Under § 103 (a)

The Office rejected claims 1-5, 15-19, 22-26, 36-40, 43-47, and 57-61 under 35 U.S.C. § 103 (a) as being obvious over U.S. Patent Application Publication 2004/0003279 to Beilinson, *et al.* in view of U.S. Patent Application Publication 2003/0217287 to Kruglenko.

These claims, however, are not obvious over *Beilinson* with *Kruglenko*. These claims recite, or incorporate, features that are not disclosed or suggested by *Beilinson* with *Kruglenko*. All the independent claims, for example, similarly recite "*intercept a message for opening a window associated with a requested computer application, the message intercepted before receipt thereof by an operating system* to prevent opening the window" (emphasis added). All the independent claims also similarly recite "*when the requested computer application is matched to the list of restricted computer applications, then prohibit opening the window associated with the requested computer application* and automatically terminate *the requested computer application*" (emphasis added). Support may be found at least at paragraphs [0061] and [0062] of the as-filed specification. Independent claim 1 is reproduced below, and independent claims 22 and 43 recite similar features.

1. A system for controlling computer access, the system operative to:

control access to use of the computer according to settings specified by an administrator for at least one user of the computer, wherein the administrator can input

changes to the settings locally to the computer and remotely from the computer on another computer to which the settings do not apply;

store a list of restricted computer applications;

intercept a message for opening a window associated with a requested computer application, the message intercepted before receipt thereof by an operating system to prevent opening the window;

compare the requested computer application to the list of restricted computer applications;

when the requested computer application is matched to the list of restricted computer applications, then prohibit opening the window associated with the requested computer application and automatically terminate the requested computer application; and

collect information from the computer on which local computer applications the respective user is attempting to access on the computer, the information being compiled in a report regarding the respective user, the report being made accessible to the administrator from a remote database.

Beilinson with *Kruglenko* does not teach or suggest all these features. As the Assignee explains below, the Office is, very respectfully, mistaken in its interpretation of both *Beilinson* and *Kruglenko*. The Office's interpretation of both *Beilinson* and *Kruglenko*, in fact, is counter to their express teachings. So, when *Beilinson* and *Kruglenko* are properly interpreted, the proposed combination of *Beilinson* and *Kruglenko* does not obviate the pending claims.

The Office, for example, has misinterpreted *Beilinson*. The Office alleges that *Beilinson* teaches "*prohibiting opening the window associated with the requested computer application and automatically terminate the requested computer application*," and the Office cites to several of *Beilinson's* paragraphs. While *Beilinson* discusses access restrictions, though, no where does *Beilinson* teach or suggest the claimed mechanism of "*prohibiting opening the window associated with the requested computer application and automatically terminate the requested computer application*," as the independent claims all similarly recite. When *Beilinson* is properly interpreted, *Beilinson* makes no such teaching.

The Office, for example, cites to *Beilinson's* paragraph [0007]. This paragraph is reproduced below.

> [0007] Once the invention is integrated into a computer system, an administrator configures user authorization settings for all users. Examples of computer functions include executing software applications such as word processors or games, playing CDs and DVDs, and storing data such as on 3.5" disk drives, writable CDs, and hard disk drives. The user authorization settings assigned to the user by the administrator on a computer are capable of being replicated on another computer and are intended to follow the user from computer to computer in the local network.

See U.S. Patent Application Publication 2004/0003279 to Beilinson, *et al.* at paragraph [0007]. This paragraph broadly discusses user authorization settings. *Beilinson's* paragraph [0007], quite simply, is entirely silent to "*prohibiting opening the window associated with the requested computer application and automatically terminate the requested computer application.*" Any other interpretation is unreasonable.

The Office also cites to *Beilinson's* paragraph [0009], which is reproduced below.

> [0009] An administrator may also restrict a user's access to specific computer functions. The invention allows an administrator the ability to deny a user all computer functions except those specifically enabled by the administrator. This effectively controls new functions that are added after the administrator configures the system. In addition, the administrator may restrict a user's access to computer functions based on several factors including time of day, elapsed process time for a specific computer function, and content rating of the requested computer function. In this regard, the content rating controls whether the user may access the computer function. An administrator may temporarily restrict access to a specific computer function, which involves disabling a user's access to the function and determining when access to the function will be automatically restored.

See U.S. Patent Application Publication 2004/0003279 to Beilinson, *et al.* at paragraph [0009]. This paragraph broadly discusses access restrictions based on time and content. Still, though, *Beilinson's* paragraph [0009] is entirely silent to "*prohibiting opening the window associated*

with the requested computer application and automatically terminate the requested computer application." Any other interpretation is unreasonable.

The Office also cites to *Beilinson's* paragraph [0054], which is reproduced below.

> [0054] As stated above, restriction component 214 can be used to restrict specific computer functions 226. The specific computer functions category 226 includes a number of sub-categories. For example, and without limitation, the sub-categories can include function name 234, time of day 236, content rating 238 and duration per day 240. The embodiment may default to denying the user access to any computer function that is not on a computer function list.

See U.S. Patent Application Publication 2004/0003279 to Beilinson, *et al.* at paragraph [0054]. This paragraph discusses computer function restrictions based on categories. Again, though, *Beilinson's* paragraph [0054] is entirely silent to "*prohibiting opening the window associated with the requested computer application and automatically terminate the requested computer application*." Any other interpretation is unreasonable.

The Office also cites to *Beilinson's* paragraph [0055], which is reproduced below.

> [0055] Function name sub-category 234 is used to deny or enable a user access to computer functions. In one implementation, for example, access is denied to all computer functions except those specifically enabled in the settings. This implementation controls new functions that are added after the administrator configures the system by denying access. Initially, a list is created that includes all computer functions. Each function on the list can be enabled or disabled by the administrator. As one who is skilled in the art will understand, this could be accomplished in a variety of ways. For example, to create a list of available applications for a computer, directories can be searched to gather executable file names, a list maintained by the operating system such as the WINDOWS Add/Remove Programs list can be used, or other methods can be employed. The list of available computer functions such as applications can also be presented in many ways. For example, the list could be presented in a window with enable and disable radio buttons, or with check boxes to enable a specific function, or in any of a number of other fashions.

See U.S. Patent Application Publication 2004/0003279 to Beilinson, *et al.* at paragraph [0055]. Here *Beilinson* discusses denying access to all functions except those enabled. *Beilinson's* paragraph [0055] goes on to explain how a list of available applications is created. Still, though, *Beilinson's* paragraph [0009] is entirely silent to "*prohibiting opening the window associated with the requested computer application and automatically terminate the requested computer application*." Any other interpretation is unreasonable.

So, *Beilinson* does not teach what the Office alleges. While *Beilinson* discusses access restrictions, *Beilinson* is entirely silent to "*prohibiting opening the window associated with the requested computer application and automatically terminate the requested computer application*," as the independent claims all similarly recite. When *Beilinson* is properly interpreted, *Beilinson* makes no such teaching.

The Office has also misinterpreted *Kruglenko*. The Office alleges that *Kruglenko* teaches some features of the independent claims, but the Office is again mistaken. The Office alleges, for example, that *Kruglenko* teaches "*intercepting a message for opening a window associated with a requested computer application, the message intercepted before receipt thereof by an operating system to prevent opening the window*" (emphasis added). While *Kruglenko* discusses a hook procedure, *Kruglenko's* hook procedure intercepts keyboard messages, not "*a message for opening a window*." Moreover, *Kruglenko's* hides windows associated with unapproved applications — *Kruglenko* does not prevent opening the window. So, when *Kruglenko* is properly interpreted, *Kruglenko* does not teach what the Office alleges.

The Office, for example, cites to *Kruglenko's* paragraph [0056]. This paragraph is reproduced below.

> [0056] A hook is a point in the message-handling mechanism where the message traffic is monitored in order to intercept and process certain messages before they reach their target window procedure 306. A hook chain, which is a list of pointers to application-defined callback functions called hook procedures, is maintained for each type of hook. When a message that is associated with a hook is intercepted, the system passes the message to the hook procedure referenced in the

> hook chain. The action taken by the hook procedure varies between types of hooks. The message may be changed, stopped altogether, or simply monitored.

See U.S. Patent Application Publication 2003/0217287 to Kruglenko at paragraph [0056]. While *Kruglenko's* paragraph [0056] discusses a hook procedure, this paragraph is entirely silent to a hook procedure that "*intercept]s] a message for opening a window associated with a requested computer application, the message intercepted before receipt thereof by an operating system to prevent opening the window*" (emphasis added). *Kruglenko*, in fact, only provides a single example of this hook procedure to intercept keyboard messages, not "*a message for opening a window*." *See Kruglenko*, at paragraph [0057]. The only reasonable conclusion, then, is that *Kruglenko* failed to contemplate the use of a hook mechanism to intercept messages for opening windows to restrict access to a computer application. Any other interpretation is unreasonable.

The Office also cites to *Kruglenko's* paragraph [0077]. This paragraph is reproduced below.

> [0077] After starting 500, the alert service 33 traces all events indicating that a new window is created or about to become active. The alert service 33 waits for any kind of notification or stop command 501. If a received message is not a stop command 502, and not a new window notification, 503, the service returns to waiting 501. If the message is a new window notification, the alert service 33 checks, using standard APIs, which process this window belongs to 504. If the process or a program associated with this program is approved as secure according to a list of approved processes and/or programs 37, no action is taken, and the service returns to waiting 501. If, however, the process cannot be approved in this manner, the alert service 33 **hides the window and/or suspends the process** 505. Information identifying the hidden window and/or suspended process is stored in a list 38. Preferably, the system issues an alert on screen and prompts the user for approval of the process. If the user enters an administrator password and approves the process 506, **the window is unhidden** and the suspended process is resumed 507. The process and/or its associated program is entered in the alert service's list of approved processes or programs 37, either for the remainder of this session or permanently, depending on the administrators input. The user may then interact with this process. Otherwise, if the administrator keeps the process suspended until the secure environment **shuts down or closes the program**, the alert service 33 returns to waiting for new commands or notifications 501.

See U.S. Patent Application Publication 2003/0217287 to Kruglenko at paragraph [0077] (emphasis added). Here *Kruglenko* describes a "new window notification" message for approved programs/processes. If the program/process is not approved, then the "**alert service hides the window and/or suspends the process**." The user is prompted, and if the user approves, the "**window is unhidden and the process resumes**." If the user does not approve, the program/process remains suspended **until shutdown or the program is closed**. Because *Kruglenko* "hides" and unhides a window, one must reasonably conclude that *Kruglenko* first opens the window before the window can be hidden and unhidden. The only reasonable conclusion, then, is that *Kruglenko* fails to teach or suggest "*intercept]s] a message for opening a window associated with a requested computer application, the message intercepted before receipt thereof by an operating system to prevent opening the window*" (emphasis added). *Kruglenko* cannot "*prevent opening the window*" if the window is hidden and unhidden. Any other interpretation is unreasonable.

Claims 1-5, 15-19, 22-26, 36-40, 43-47, and 57-61, then, cannot be obvious over *Beilinson* and *Kruglenko*. Independent claims 1, 22, and 43 recite many features that are not disclosed or suggested by *Beilinson* and *Kruglenko*. The respective dependent claims incorporate these same features and recite additional features. One of ordinary skill in the art, then, would not think that the pending claims are obvious over *Beilinson* with *Kruglenko*. The Office is respectfully requested to remove the § 103 (a) rejection of these claims.

Rejection of Claims Under § 103 (a) over *Beilinson, Kruglenko & Mathew*

The Office rejected claims 6-8, 11, 20-21, 27-29, 31-32, 41-42, 48-50, 52-53, and 62-63 under 35 U.S.C. § 103 (a) as being obvious over *Beilinson* and *Kruglenko* and further in view of U.S. Patent Application Publication 2004/000307 to Mathew, *et al.*

These claims, however, cannot be obvious over the proposed combination of *Beilinson*, *Kruglenko*, and *Mathew*. These claims depend, respectively from one of independent claims 1,

22, or 43. These claims, then, incorporate the same distinguishing features discussed above, and these claims recite additional features. As the above paragraphs explained, both *Beilinson* and *Kruglenko* are silent to many features recited by the independent claims, and *Mathew* does not cure these deficiencies. *Mathew* describes a history summary report that tracks a user's online and offline activities. Still, though, the combined teaching of *Beilinson*, *Kruglenko*, and *Mathew* fails to teach or suggest all the features of the independent claims. One of ordinary skill in the art, then, would not think that claims 6-8, 11, 20-21, 27-29, 31-32, 41-42, 48-50, 52-53, and 62-63 are obvious over *Beilinson*, *Kruglenko*, and *Mathew*. The Office is respectfully requested to remove the § 103 (a) rejection of these claims.

Rejection of Claims Under § 103 (a) over *Beilinson, Kruglenko, Mathew & Rowland*

The Office rejected claims 12-13, 33-34, and 54-55 under 35 U.S.C. § 103 (a) as being obvious over *Beilinson*, *Kruglenko*, and *Mathew* and further in view of U.S. Patent 6,405,318 to Rowland.

Again, though, these claims cannot be obvious over the proposed combination of *Beilinson*, *Kruglenko*, *Mathew*, and *Rowland*. These claims depend, respectively from one of independent claims 1, 22, or 43. These claims, then, incorporate the same distinguishing features and recite additional features. As the above paragraphs explained, *Beilinson*, *Kruglenko*, and *Mathew* fail to teach or suggest many features recited by independent claims 1, 22, or 43, and *Rowland* does not cure these deficiencies. *Rowland* describes a "login anomaly detection function" that logs all logins and logouts. Still, though, the combined teaching of *Beilinson*, *Kruglenko*, *Mathew*, and *Rowland* fails to teach or suggest all the features recited by independent claims 1, 22, or 43. The combined teaching of *Beilinson*, *Kruglenko*, *Mathew*, and *Rowland*, then, cannot obviate claims 12-13, 33-34, and 54-55. The Office is respectfully requested to remove the § 103 (a) rejection of these claims.

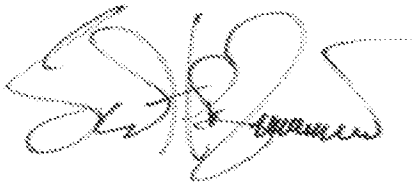
Rejection of Claims Under § 103 (a) over *Beilinson, Kruglenko, Mathew & Terry*

The Office rejected claims 14, 35, and 56 under 35 U.S.C. § 103 (a) as being obvious over *Beilinson*, *Kruglenko*, and *Mathew* and further in view of U.S. Patent Application Publication 2002/0026605 to Terry.

Again, though, these claims cannot be obvious over the proposed combination of *Beilinson*, *Kruglenko*, *Mathew*, and *Terry*. These claims depend, respectively from one of independent claims 1, 22, or 43. These claims, then, incorporate the same distinguishing features and recite additional features. As the above paragraphs explained, *Beilinson*, *Kruglenko*, and *Mathew* fail to teach or suggest many features recited by independent claims 1, 22, or 43, and *Terry* does not cure these deficiencies. *Terry* describes real-time detection of computer states, including start-up files. Still, though, the combined teaching of *Beilinson*, *Kruglenko*, *Mathew*, and *Terry* fails to teach or suggest all the features recited by independent claims 1, 22, or 43. The combined teaching of *Beilinson*, *Kruglenko*, *Mathew*, and *Terry*, then, cannot obviate claims 14, 35, and 56. The Office is respectfully requested to remove the § 103 (a) rejection of these claims.

If any issues remain outstanding, the Office is requested to contact the undersigned at (919) 469-2629 or *scott@scottzimmerman.com*.

Respectfully submitted,



Scott P. Zimmerman
Attorney for the Assignee
Reg. No. 41,390